NUI Galway
OÉ Gaillimh

Semester Two Examinations 2018/2019

Exam Code(s)	4BCT1, 1MECE1, 1OA1, 1EM1
Exam(s)	Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	No
External Examiner(s)	Dr. Jacob Howe
Internal Examiner(s)	Prof M. Madden *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	2
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	X	No	
MCQ	Yes		No	X
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes		No	X

PTO

1 (a) Define three security properties that are associated with cryptographic hash functions. (9 marks)

(b) Discuss any one application that might require second preimage resistance (8 marks)

(c) What is given by a message authentication code (MAC) that is not given by a cryptographic hash function? (8 marks)

2 (a) In an authentication scheme, what options are generally found for identifying a party and which option is commonly found with bank terminals? (5 marks)

(b) Explain how a nonce provides evidence of freshness in a communication (5 marks)

(c) Outline the operation of a zero-knowledge authentication scheme using any analogy of your own choice (15 marks)

3 (a) Provide a short overview of a simple stream cipher and explain how the plaintext is recovered from the ciphertext (listing any assumption you make for XOR) (10 marks)

(b) Distinguish between the block cipher modes of operation known as cipher feedback mode and cipher block chain in terms of how they handle encryption. Which behaves more like a stream cipher? (5 marks)

(c) Show how a padding oracle attack works on the last byte in cipher block chain decryption (10 marks)

4 (a) In terms of Public Key Infrastructure (PKI), explain what is meant by the terms 'public key' 'private key', and 'digital certificate' (9 marks)

(b) Differentiate between encryption services and signing services (8 marks)

(c) Briefly explain the purpose of DNSSEC, Registry Lock, Certificate Transparency Logs, Extensible Provisioning Protocol (8 marks)

5 (a) In the context of computer forensics, explain what is meant by the Daubert criteria (9 marks)

(b) What is meant by the term 'steganography' and list any three environments where it could be found? (8 marks)

(c) How does steganalysis help with steganography? List any two approaches an administrator might deploy to help with steganography? (8 marks)

6

By considering the recent paper in ACM Queue by Waldo, or otherwise, discuss Blockchain under the headings:
(a) ledger (5 marks)
(b) reward (5 marks)
(c) trusted versus trustless systems (15 marks)